pwc

Cybercrime Survey 2025

November 2025

Indhold

86 %

af virksomhederne med en øget bekymring for cybertrusler relaterer denne til den geopolitiske situation.

76 %

af virksomhedernes bestyrelser har cybersikkerhed som en fast del af deres årshjul.

50 %

af virksomhederne oplever, at manglende overblik over tredjeparter og leverandører er den største barriere for at leve op til de nye sikkerhedskrav i NIS 2 og DORA.

64 %

af respondenterne forventer, at deres virksomheds cyber- og informationssikkerhedsbudget vil vokse inden for de næste 12 måneder.

Cybercrime Survey 2025 er baseret på besvarelser fra 405 ledere, sikkerhedsansvarlige og fagspecialister fra både den offentlige og den private sektor. Undersøgelsen giver et aktuelt indblik i investeringer, udfordringer og strategiske prioriteringer inden for cybersikkerhed. Respondenterne har desuden bidraget med vurderinger af det nuværende trusselsbillede samt med indblik i, hvordan og i hvilket omfang der arbejdes med cyber- og informationssikkerhed på tværs af sektorer.

Cyber-sikkerhed i en kompleks verden: Øget fokus på leverandør-styring og regulatorisk tilpasning

Geopolitiske spændinger driver øget beredskabsfokus

Den geopolitiske situation præger trusselsbilledet og påvirker bekymringen for cyberangreb. 86 % af de virksomheder, der oplever øget bekymring, nævner konfliktspændinger – især i relation til USA og Rusland – som hovedårsagen. Som følge af konfliktspændingerne og den stigende bekymring om cybersikkerhed har 40 % af alle virksomhederne allerede iværksat specifikke forebyggende og afhjælpende cybersikkerhedstiltag. Denne udvikling viser, at virksomheder i dag må indrette sig efter en kompleks og uforudsigelig sikkerhedssituation, hvor stabilitet og robusthed sættes i højsædet.

Leverandørstyring – en afgørende brik i cybersikkerhed

Årets undersøgelse viser, at virksomheder i stigende grad erkender vigtigheden af en omfattende leverandørstyring i sikringen af deres digitale modstandskraft. Halvdelen af de adspurgte virksomheder peger på manglende overblik over tredjeparter og leverandører som en væsentlig barriere for at overholde de nye krav i NIS 2 og DORA. Behovet for styrket kontrol og transparens på tværs af forsyningskæden er dermed større end nogensinde.

Teknologiske investeringer og regulatorisk tilpasning rykker frem

Investeringerne i cyber- og informationssikkerhed fortsætter med at vokse, og flere virksomheder forankrer indsatsen i organisationen og ledelsen. Samtidig er der forsat fokus på kendskabet til de nye regulatoriske krav i NIS 2 og DORA, og en stor del af virksomhederne er i gang med implementeringen. Denne øgede regulatoriske bevidsthed og indsats bidrager til et styrket fokus på operationel modstandsdygtighed og langsigtet risikostyring.

Et samlet blik fremad

Årets Cybercrime Survey viser, at danske organisationer arbejder mere målrettet med cybersikkerhed. Arbejdet drives især af geopolitiske risici og de nye reguleringer, der stiller større krav til både kontrol og dokumentation. At imødekomme disse krav og styrke modstandsdygtigheden kræver en bred forankring af cybersikkerheden, både internt i organisationen og eksternt i leverandørkæden. En effektiv tilgang forudsætter, at indsatsen prioriteres, ud fra hvad der er mest kritisk for virksomhedens fortsatte drift.

40 %

har som følge af globale konfliktspændinger allerede iværksat specifikke forebyggende og afhjælpende cybersikkerhedstiltag.

Christian Kjær
Partner
Cyber & Privacy

Cyber-sikkerhed i fokus

Danske virksomheder og offentlige organisationer opruster fortsat på cybersikkerhedsområdet.

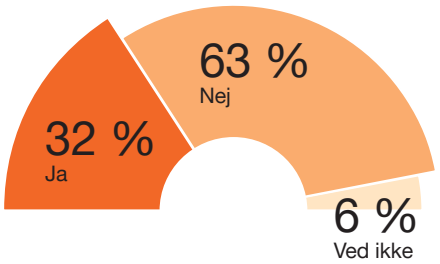
62 %

af de virksomheder, der har været ramt af sikkerhedshændelser, rapporterer, at det drejer sig om phishingangreb.

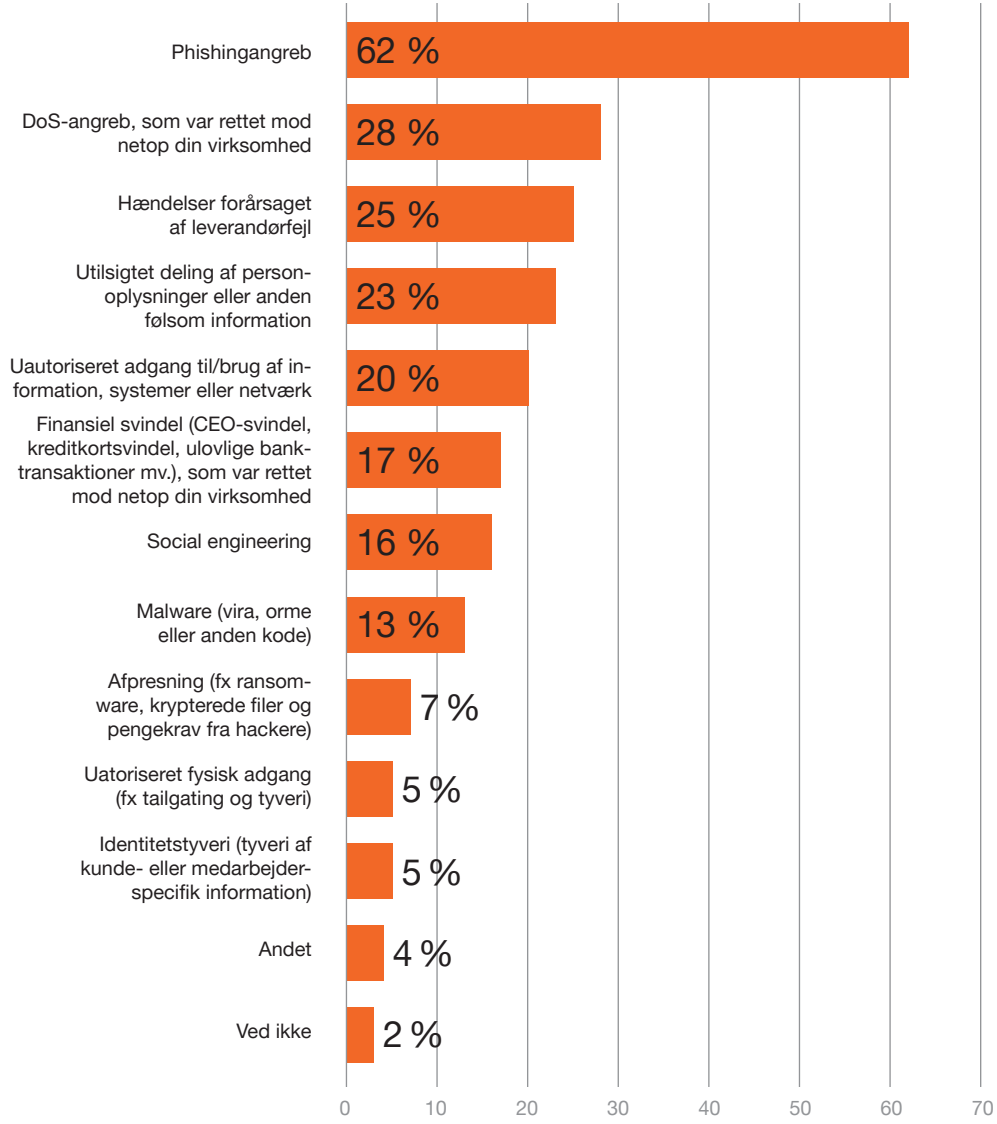
Danske virksomheder og offentlige organisationer opruster fortsat på cybersikkerhedsområdet. Dette års Cybercrime Survey viser, at selvom kun hver tredje virksomhed har oplevet en konkret sikkerhedshændelse det seneste år, er cybersikkerhed stadig blandt de mest prioriterede investeringsområder.

Blandt de virksomheder, der har været ramt, er phishingangreb den mest udbredte type hændelse, idet 62 % af virksomhederne rapporterer at have været udsat for denne form for angreb. Derudover er DoS-angreb, leverandørfejl og utilsigtet deling af følsomme oplysninger hyppigt forekommende hændelser, som henholdsvis 28 %, 25 % og 23 % af virksomhederne har oplevet.

Har din virksomhed været udsat for en sikkerhedshændelse inden for de seneste 12 måneder?



Hvilken type sikkerhedshændelse(r) var der tale om?

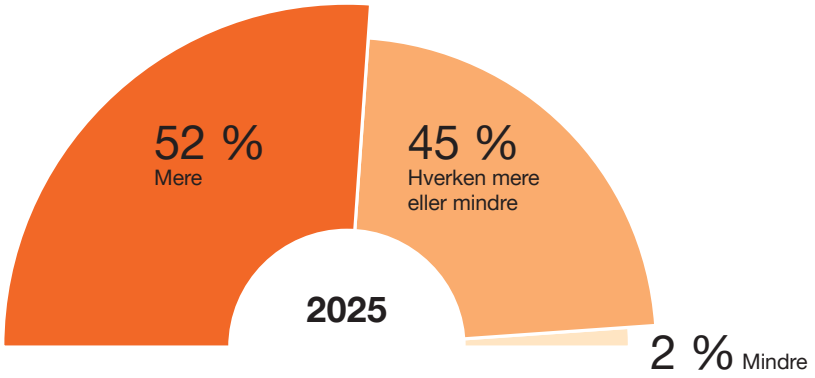


Samtidig angiver 52 % af respondenterne, at de er mere bekymrede for cybertrusler nu end for 12 måneder siden. Når det gælder bekymring for de mest alvorlige konsekvenser, nævner 72 % længerevarende nedbrud på kritiske systemer som deres største frygt, 56 % peger på økonomiske tab, og 46 % bekymrer sig mest om kompromittering af fortrolige oplysninger.

72 %

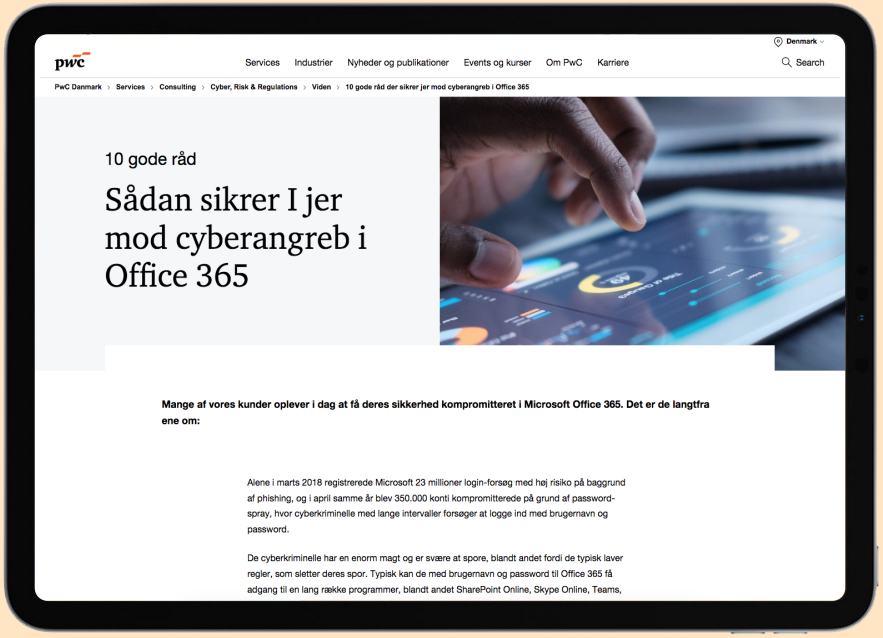
af respondenterne er mest bekymret for længerevarende nedbrud på kritiske systemer som en alvorlig konsekvens af cybertrusler.

Bekymrer du dig i dag mere eller mindre om de cybertrusler, din virksomhed oplever, end du gjorde for 12 måneder siden?



Phishing

Phishing er en form for it-kriminalitet, hvor cyberkriminelle forsøger at narre dig til at afgive fortrolige oplysninger såsom brugernavne og adgangskoder. Dette foregår ofte via e-mails, der efterligner legitime beskeder fra velkendte organisationer, men som i virkeligheden har til formål at stjæle dine data. Hvis en medarbejder klikker på et ondsindet link eller åbner en vedhæftet fil, kan det give de kriminelle adgang til følsomme oplysninger eller skabe en bagdør ind i virksomhedens it-systemer. Den bedste beskyttelse mod phishing er øget opmærksomhed og en kritisk tilgang til alle uopfordrede henvendelser, især når der bliver bedt om personlige eller fortrolige oplysninger.



Besøg PwC's hjemmeside for at få mere information om, hvordan du kan beskytte dig selv mod phishing.

Investeringerne vokser, og det gør ambitionsniveauet også

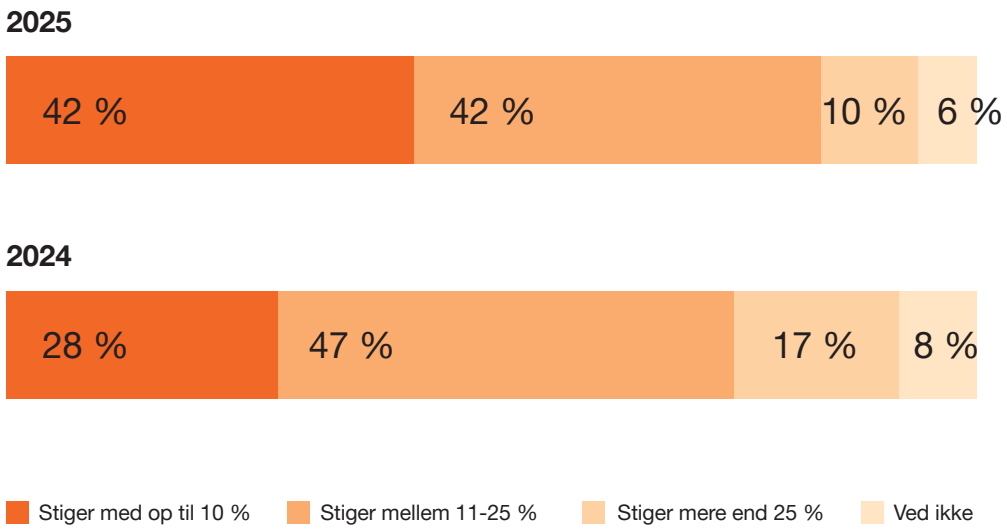
Cybersikkerhed er ikke længere et spørgsmål om, hvorvidt man skal investere, men hvordan investeringerne skal fordeles og prioriteres.

64 %

af respondenterne forventer, at deres budget til cyber- og informationssikkerhed vil vokse i løbet af de næste 12 måneder.

Når man sammenligner forventningerne til cybersikkerhedsbudgetterne for 2024 og 2025, tegner der sig et billede af en ændret investeringsstrategi. I 2024 forventede 47 % af respondenterne en vækst i budgettet på 11-25 %, og 28 % forudså en stigning på 1-10 %. I 2025 fremstår billedet mere afdæmpet og balanceret, hvor 42 % forventer en vækst på 11–25 %, og ligeledes 42 % i kategorien 1–10 %, mens kun 10 % forventer stigninger over 25 %. Dette kan indikere, at en stor del af det nødvendige arbejde med at imødekomme kravene fra NIS 2 og DORA allerede er gennemført, hvilket har medført, at budgetstigningerne nu er tilbage på et mere normalt niveau.

Hvor meget forventer du, at cyber- og informationssikkerhedsbudgettet vil stige inden for de næste 12 måneder?



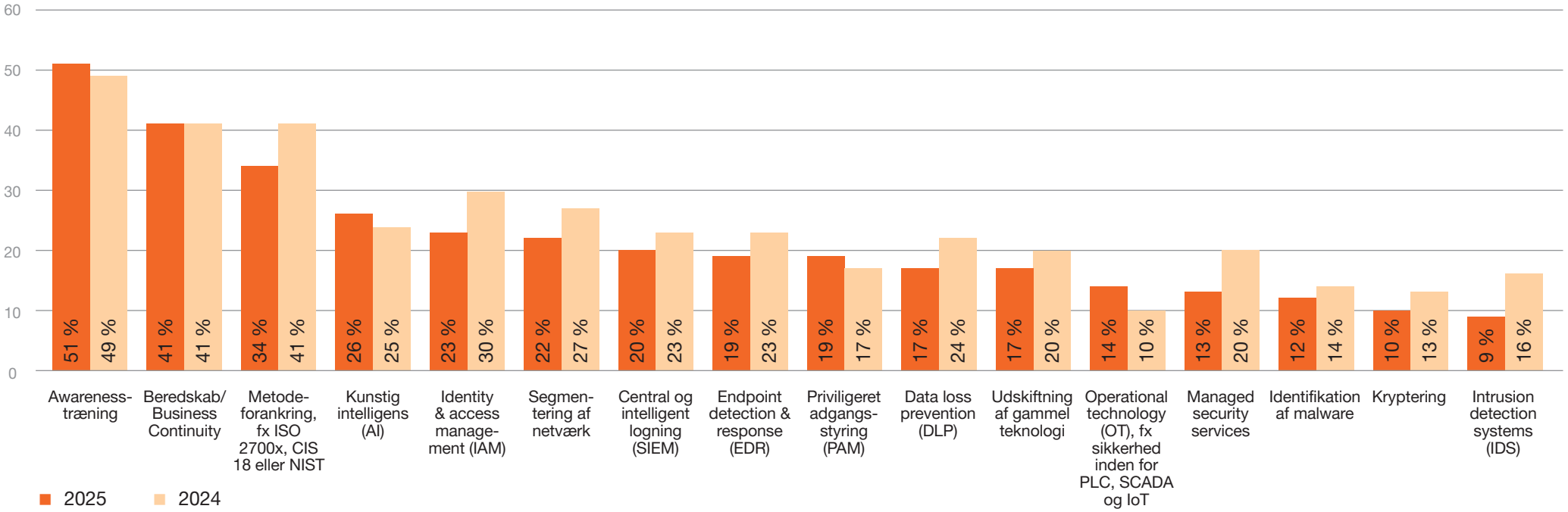
De områder, der tiltrækker de største investeringer, omfatter awareness-træning, som 51 % af virksomhederne prioriterer højt, efterfulgt af beredskab med 41 % og metodeforankring, som 34 % af organisationerne fokuserer på. Denne fordeling understreger en helheds-orienteret tilgang, hvor både forebyggelse, evnen til at reagere på hændelser og organisatorisk forankring vægtes højt.

Derudover udgør investeringer i teknologiske løsninger en væsentlig del af virksomhedernes cybersikkerheds-indsats, hvor bl.a. kunstig intelligens og netværkssegmentering – prioriteret af henholdsvis 26 % og 22 % af virksomhederne – illustrerer, hvordan digital innovation fortsat spiller en central rolle i cybersikkerhedsstrategien.

41 %

af virksomhederne i undersøgelsen prioriterer investeringer i beredskab og 34 % i metodeforankring, hvilket understreger en helhedsorienteret tilgang.

Hvad er din virksomheds højst prioriterede investeringer inden for cyber- og informationssikkerhed de næste 12 måneder?



PwC erfarer

Awareness-træning er en nødvendig og effektiv metode til at styrke medarbejdernes forståelse af cybersikkerhed og reducere virksomhedens samlede sikkerhedsrisiko.

PwC oplever, at de mest succesfulde virksomheder integrerer løbende e-læring som en fast del af medarbejderuddannelsen, hvor træningen tilpasses forskellige roller og niveauer i organisationen.

Ved at fokusere på relevante, praksisnære scenarier og interaktive læringsmetoder øges medarbejdernes evne til at genkende og reagere korrekt på cybertrusler som phishing og social engineering. Samtidig skal awareness-indsatsen understøttes af ledelsens prioritering og kontinuerlig kommunikation, så cybersikkerhed bliver en del af virksomhedskulturen.

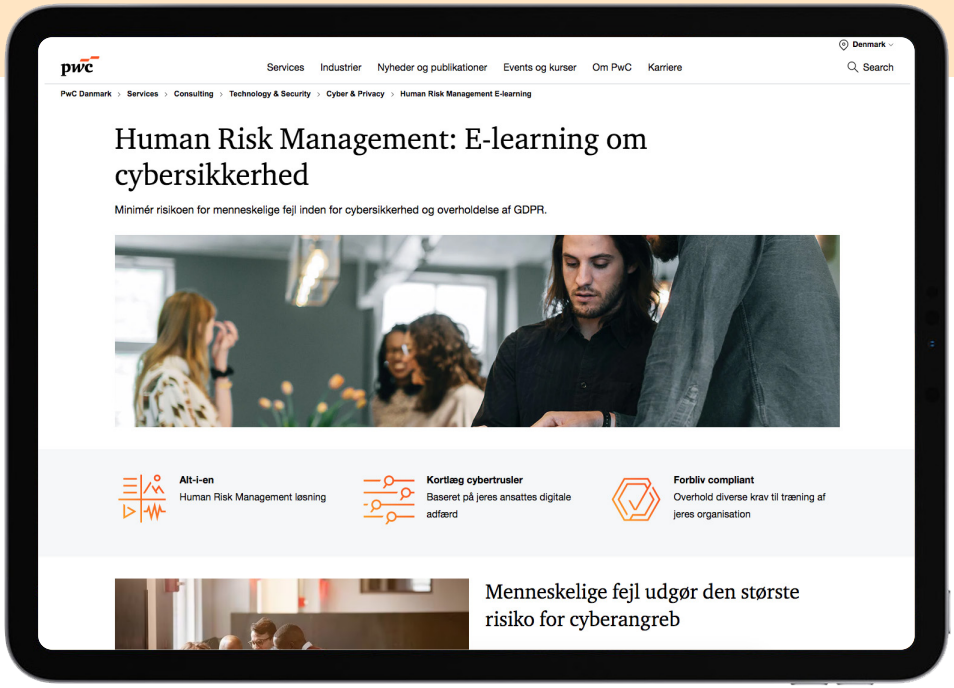
PwC anbefaler en systematisk og målrettet tilgang til awareness-træning, der løbende evalueres og justeres i takt med de skiftende trusler og organisationens behov.

Læs mere om PwC's tilgang til e-læring og cybersikkerheds-træning.

> PwC oplever, at de mest succesfulde virksomheder integrerer løbende e-læring som en fast del af medarbejder-uddannelsen, hvor træningen tilpasses forskellige roller og niveauer i organisationen.

51 %

af virksomhederne i undersøgelsen prioriterer investeringer i awareness-træning inden for cyber- og informationssikkerhed.



Geopolitik som drivkraft for cyber-sikkerhed

Den stigende bekymring for cybertrusler hænger tæt sammen med den aktuelle geopolitiske situation, hvor krigen mellem Rusland og Ukraine har intensiveret spændingerne mellem Rusland, Europa og USA.

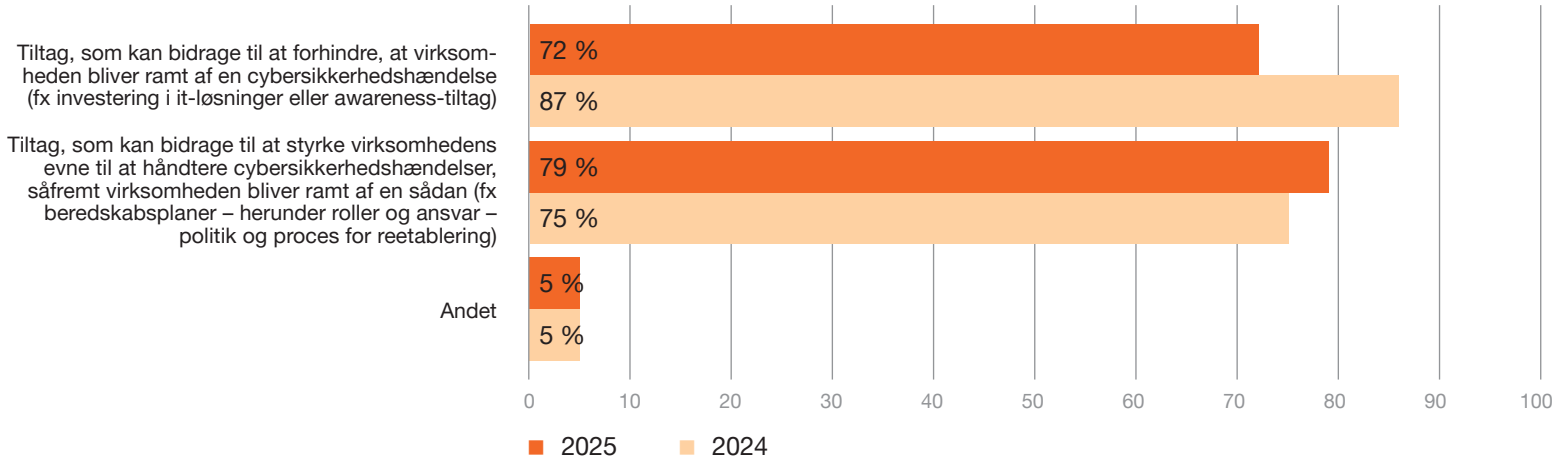
86 %

af de respondenter, der oplever øget bekymring for cybertrusler, tilskriver denne bekymring kompleksitet og usikkerhed på internationalt plan.

Hele 86 % af de respondenter, der oplever øget bekymring, tilskriver den netop kompleksitet og usikkerhed på det internationale plan. Som følge heraf har 40 % af alle virksomhederne allerede implementeret nye cybersikkerhedstiltag.

Blandt disse virksomheder prioriterer 79 % beredskab, og 72 % fokuserer på forebyggelse. Dette viser, at mange organisationer arbejder med flere typer af tiltag og dermed har en helhedsorienteret tilgang til cybersikkerhed.

Hvilke nye cybersikkerhedstiltag har din virksomhed implementeret som følge af den øgede bekymring for cybertrusler?



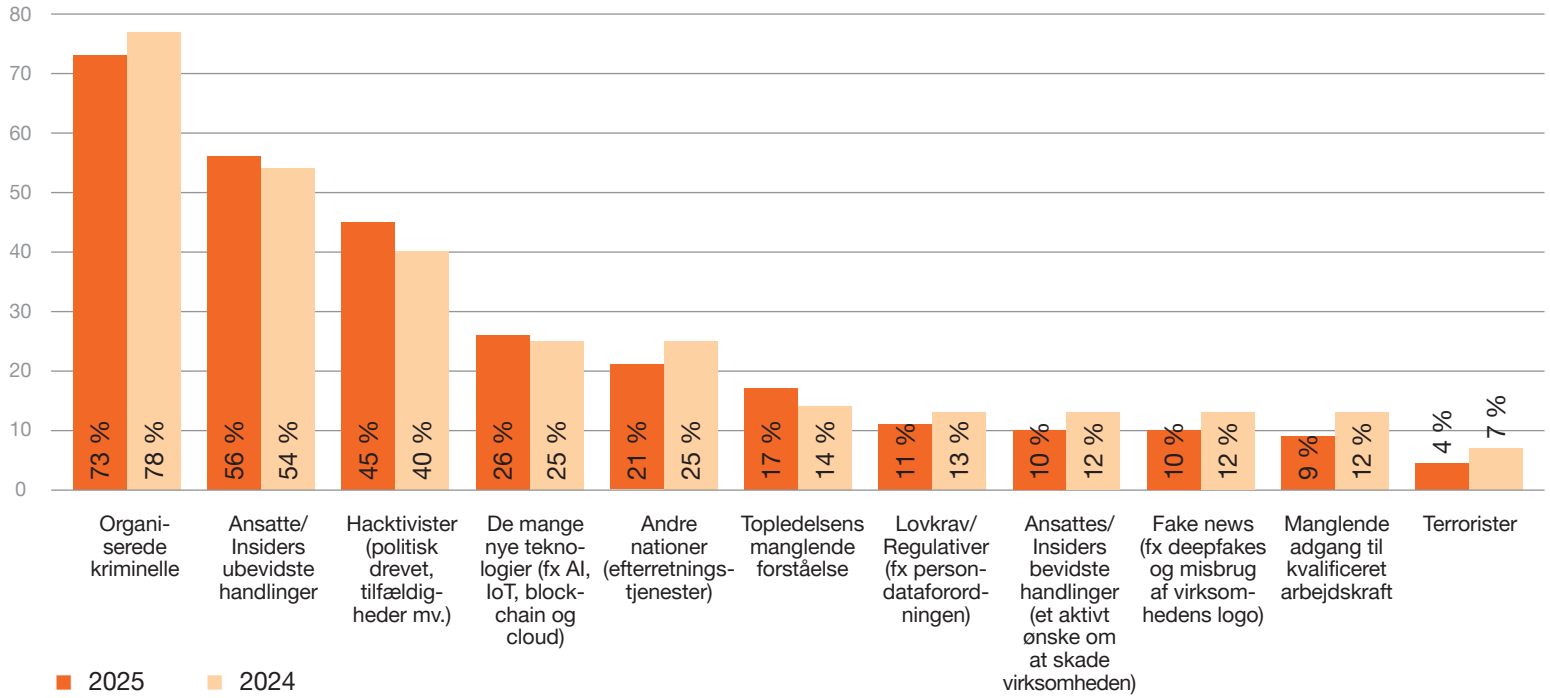
73 %

af respondenterne angiver organiserede kriminelle som den største trussel i relation til cyber- og informationssikkerhed.

Ligesom i 2024 udgør organiserede kriminelle med 73 % den største trussel mod virksomhedernes cyber- og informationssikkerhed. Dernæst følger ubevidste handlinger fra ansatte (56 %) og hacktivister med politiske eller ideologiske motiver (45 %).

De mange nye teknologier som AI, IoT og cloud ses også som en kilde til øget risiko (26 %). Resultaterne understreger, at truslerne både kommer udefra og indefra, og at medarbejdernes adfærd spiller en central rolle i virksomhedernes sikkerhedsbillede.

Hvad udgør de største trusler for din virksomhed i relation til cyber- og informationssikkerhed?



> Resultaterne understreger, at truslerne både kommer udefra og indefra, og at medarbejdernes adfærd spiller en central rolle i virksomhedernes sikkerhedsbillede.

Det er vigtigt at etablere beredskabsevner, der omfatter it, krisehåndtering og nødplaner i forretningen – inklusive evnen til at kommunikere effektivt med kunder, myndigheder og øvrige interessenter.

PwC erfarer

Den aktuelle geopolitiske situation øger risikoen for avancerede cyberangreb, som kan ramme virksomheder på tværs af sektorer og landegrænser. PwC anbefaler derfor, at virksomheder styrker deres beredskab i forhold til at sikre kontinuiteten af kritiske forretningsgange.

Det kræver et tæt samarbejde mellem ledelsen, sikkerhedsteamet og forretningsenhederne at identificere og kvalificere, hvilke aktiver og leverandører der understøtter det vigtigste i forretningen. Det er vigtigt at etablere beredskabsevner, der omfatter it, krisehåndtering og nødplaner i forretningen – inklusive evnen til at kommunikere effektivt med kunder, myndigheder og øvrige interessenter. Beredskabsevnerne bør vedligeholdes og trænes regelmæssigt for at forankre dem i organisationen.

Virksomheder bør desuden gennemgå sikkerheden i deres leverandørkæder for at minimere sårbarheder og sikre, at tredjepartsadgang til systemer og data er tilstrækkeligt kontrolleret.

Endelig kræver den øgede trusselsrisiko et stærkt engagement fra både bestyrelsen og ledelsen, som skal prioritere cybersikkerhed i virksomhedens strategiske beslutninger og sikre løbende rapportering om sikkerhedstilstanden. PwC anbefaler en samlet og proaktiv tilgang for at styrke modstandskraften over for de komplekse cybertrusler, der opstår i kølvandet på geopolitiske konflikter.

Læs mere om PwC's anbefalinger til håndtering af geopolitiske cybertrusler og om, hvordan vi kan hjælpe dig.

NIS 2 og DORA fastholder momentum

Arbejdet med at imødekomme kravene i de nye EU-reguleringer, NIS 2-direktivet og DORA-forordningen, fortsætter med høj intensitet blandt danske virksomheder. Årets undersøgelse viser, at reguleringerne stadig har stor strategisk betydning, selvom de ikke længere fylder så meget i den offentlige debat.

13 %

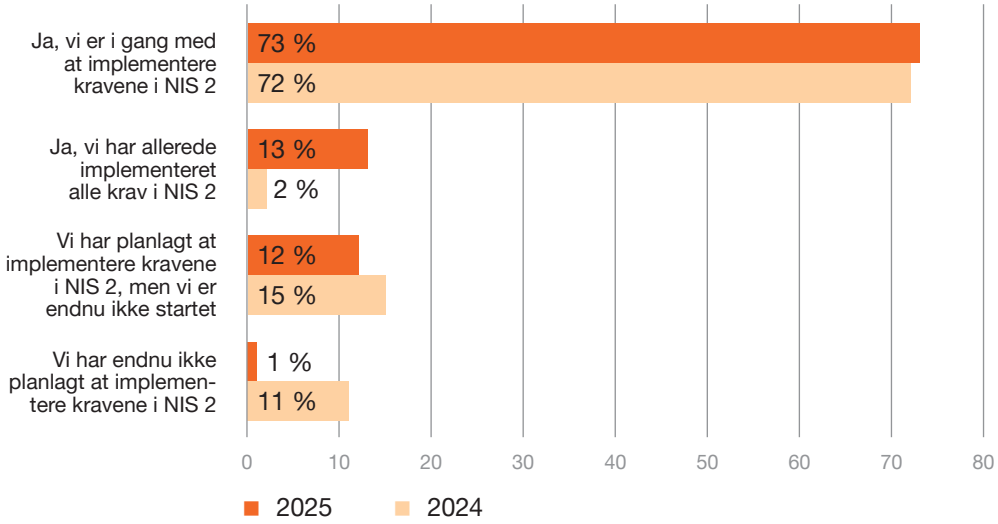
af de adspurgte virksomheder har allerede implementeret alle krav i NIS 2, og 73 % er i gang.

NIS 2: Fra kendskab til implementering

Kendskabet til NIS 2-direktivet blandt virksomhederne er uændret i forhold til 2024, hvor 80 % af de adspurgte, der er omfattet af forordningen, angav at være fuldt bekendt med direktivets krav og betydning. Knap tre ud af fire virksomheder er i gang med at implementere kravene i NIS 2-direktivet, hvilket er på niveau med 2024.

Der er dog sket et markant spring opad, når det kommer til andelen af virksomheder, som har implementeret kravene. Den er steget fra 2 % i 2024 til 13 % i 2025, hvilket vidner om, at flere virksomheder prioriterer at opnå compliance for at styrke deres cybersikkerhed og sikre overholdelse af gældende lovgivning.

Har din virksomhed* en plan for, hvordan I vil imødekomme/implementere kravene i NIS 2-direktivet?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

Virksomhedernes implementeringsplaner for NIS 2 omfatter gennemførelse af gap-analyser, som 80 % har inkluderet som en del af deres proces, udarbejdelse af en implementeringsstrategi, som 68 % har prioriteret, samt fastlæggelse af scope, som 71 % arbejder på at definere.

De primære barrierer for at kunne leve op til NIS 2-kravene er ifølge 49 % af virksomhederne udfordringer med sikkerheden i forsyningskæden, mens 42 % peger på mangelfuld risikostyring. Disse barrierer understreger behovet for tværgående samarbejde og øget teknologisk modenhed for at sikre effektiv implementering.

49 %

peger på udfordringer med sikkerheden i forsyningskæden som barriere for at kunne leve op til kravene i NIS 2-direktivet.

NIS 2-direktivet

NIS 2-direktivet (Network and Information Systems Directive 2) er EU's opdaterede regelsæt for cybersikkerhed, som har til formål at styrke beskyttelsen af kritisk infrastruktur og digitale tjenester på tværs af medlemslandene. Direktivet stiller skærpede krav til virksomheder og offentlige myndigheder inden for bl.a. energiproduktion, transport, sundhed og digitale infrastrukturer.

NIS 2 øger ansvaret for ledelsen og indfører strengere krav til risikostyring, hændelsesrapportering og sikkerhedsforanstaltninger. Formålet er at skabe en høj og ensartet cybersikkerhedsstandard, der kan modstå stadig mere komplekse trusler og sikre samfundets digitale stabilitet.

> Årets undersøgelse viser, at reguleringerne stadig har stor strategisk betydning, selvom de ikke længere fylder så meget i den offentlige debat.

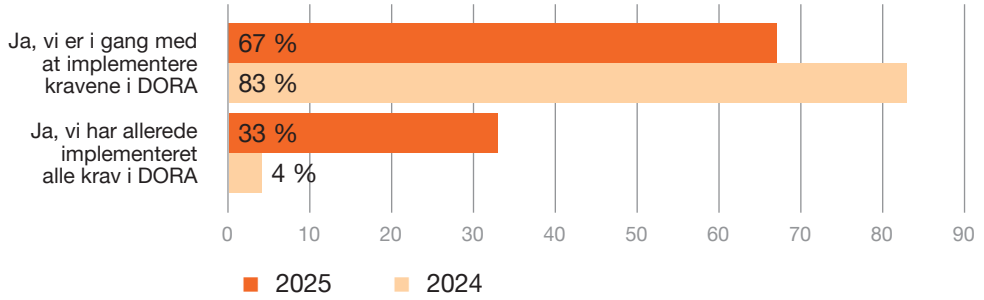
DORA: Kendskab og implementering

Kendskabet til DORA-forordningen er på niveau med sidste år, idet hele 95 % af respondenterne, der er omfattet af forordningen, er fuldt bekendt med kravene. Dog er der i år markant flere virksomheder, som har fået implementeret alle krav i DORA sammenlignet med 2024.

Implementeringen af DORA involverer forskellige dele af organisationerne, hvor ledelsen er engageret i 83 % af tilfældene, compliance-funktionerne spiller en central rolle i 72 % af virksomhederne, og risk-afdelingerne er aktive i 67 % af implementeringsprojekterne.

Barriererne for implementeringen af DORA ligner i høj grad udfordringerne ved NIS 2. Manglende overblik over tredjeparter og leverandører udfordrer 50 % af virksomhederne, mens mangler i risikostyringen opleves som en barriere af 28 %. Dette afspejler, at både NIS 2 og DORA stiller krav, som kræver øget fokus på leverandørstyring og effektiv risikohåndtering.

Har din virksomhed* en plan for, hvordan I vil imødekomme/implementere kravene i DORA-forordningen?



*) Kun virksomheder, der har angivet, at de er omfattet af DORA.

PwC erfarer

Implementeringen af DORA (Digital Operational Resilience Act) stiller nye og omfattende krav til finanssektoren, hvor virksomhederne skal sikre en høj grad af operationel modstandsdygtighed over for it-relaterede risici. PwC oplever, at compliance i forhold til DORA kræver en tværgående indsats, hvor både it, risikostyring og ledelse skal samarbejde om at etablere robuste processer for risikoidentifikation, test af it-systemer og håndtering af hændelser.

En struktureret tilgang til leverandørstyring og kontinuitetsplanlægning er ligeledes afgørende for at leve op til lovgivningens krav om transparens og beredskab. PwC anbefaler, at virksomheder arbejder proaktivt med at integrere DORAs krav i eksisterende governance- og sikkerhedsrammer, samt at de løbende evaluerer og dokumenterer deres compliance-tiltag for at styrke den digitale robusthed og undgå sanktioner.

Læs mere om PwC's anbefalinger til DORA-compliance.

> 95 % af respondenterne, der er omfattet af DORA-forordningen, er fuldt bekendt med kravene. Dog er der i år markant flere virksomheder, som har fået implementeret alle krav i DORA sammenlignet med 2024.

Anvender din virksomhed leverandører i forbindelse med kritiske it-systemer?

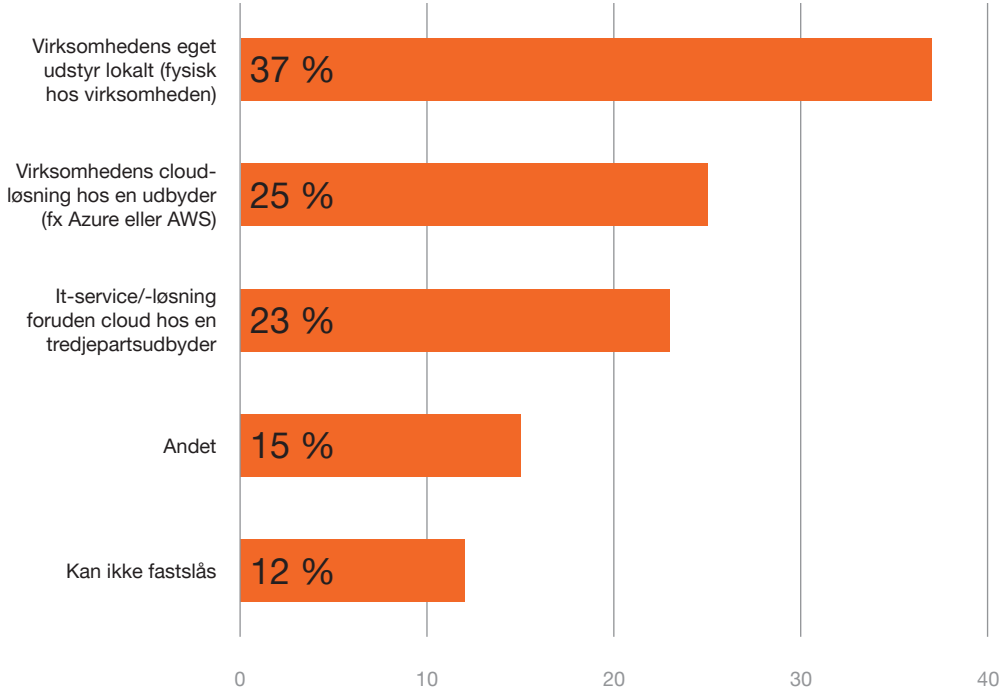
Outsourcing af en virksomheds it-infrastruktur indebærer en afgivelse af kontrol og et indskrænket ansvar for cybersikkerheden.

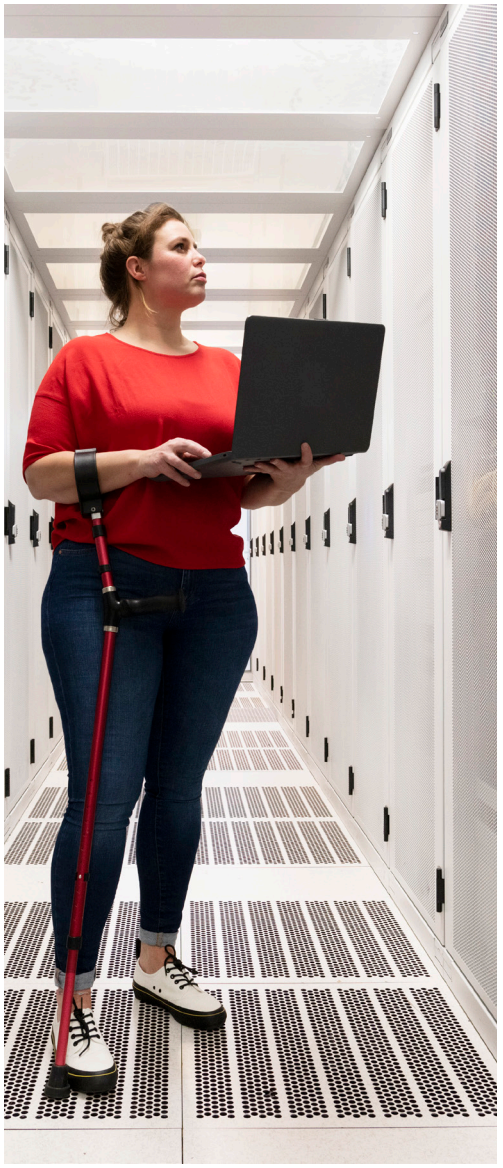
25 %

af respondenterne angiver, at en sikkerheds-hændelse målrettet mod deres virksomhed har involveret virksomhedens cloud-løsning hos en tredjepartsudbyder.

Outsourcing af en virksomheds it-infrastruktur medfører reduceret kontrol, da eksterne leverandører skaber en fragmenteret struktur med begrænset gennemsigtighed, hvilket gør det vanskeligere at identificere og håndtere risici. Samtidig øger reguleringer som NIS 2 presset på virksomhederne, der i stigende grad skal sikre, at hele deres leverandørkæde lever op til kravene i direktivet. 25 % af respondenterne angiver, at en sikkerhedshændelse målrettet mod deres virksomhed har involveret virksomhedens cloud-løsning hos en tredjepartsudbyder. Det er et fald fra 33 % i 2024 og indikerer en positiv udvikling.

Hvad var sikkerhedshændelsen, som var målrettet din virksomhed, relateret til?



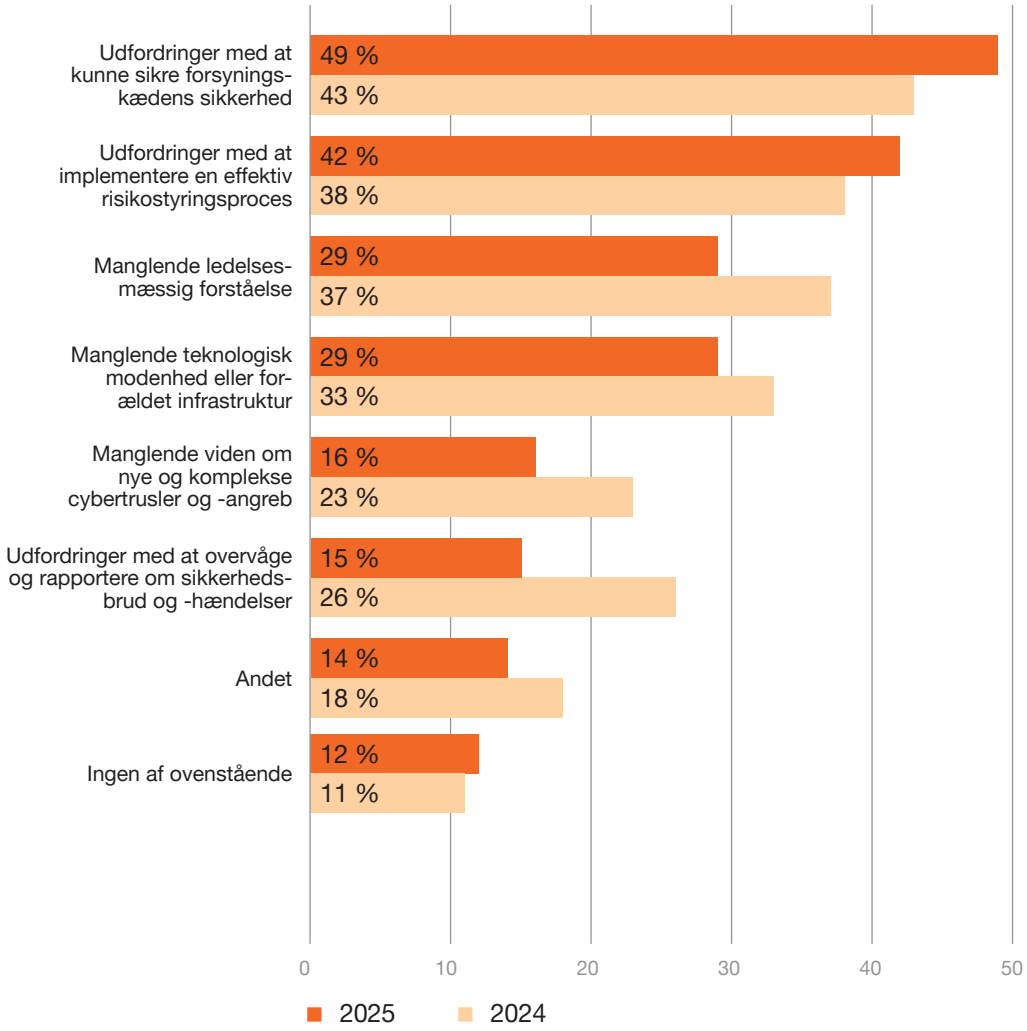


Forsyningskæden som barriere for overholdelse af NIS 2- og DORA-krav

50 % af respondenterne angiver, at manglende overblik over tredjeparter og outsourcing-leverandører er den største barriere for at leve op til kravene i DORA, hvilket er en stigning fra 35 % i 2024. Samtidig angiver 49 % af respondenterne, at udfordringer med forsyningskædens sikkerhed udgør en væsentlig barriere for at leve op til kravene i NIS 2. Det er en stigning fra 43 % i 2024 og afspejler en øget opmærksomhed på området.

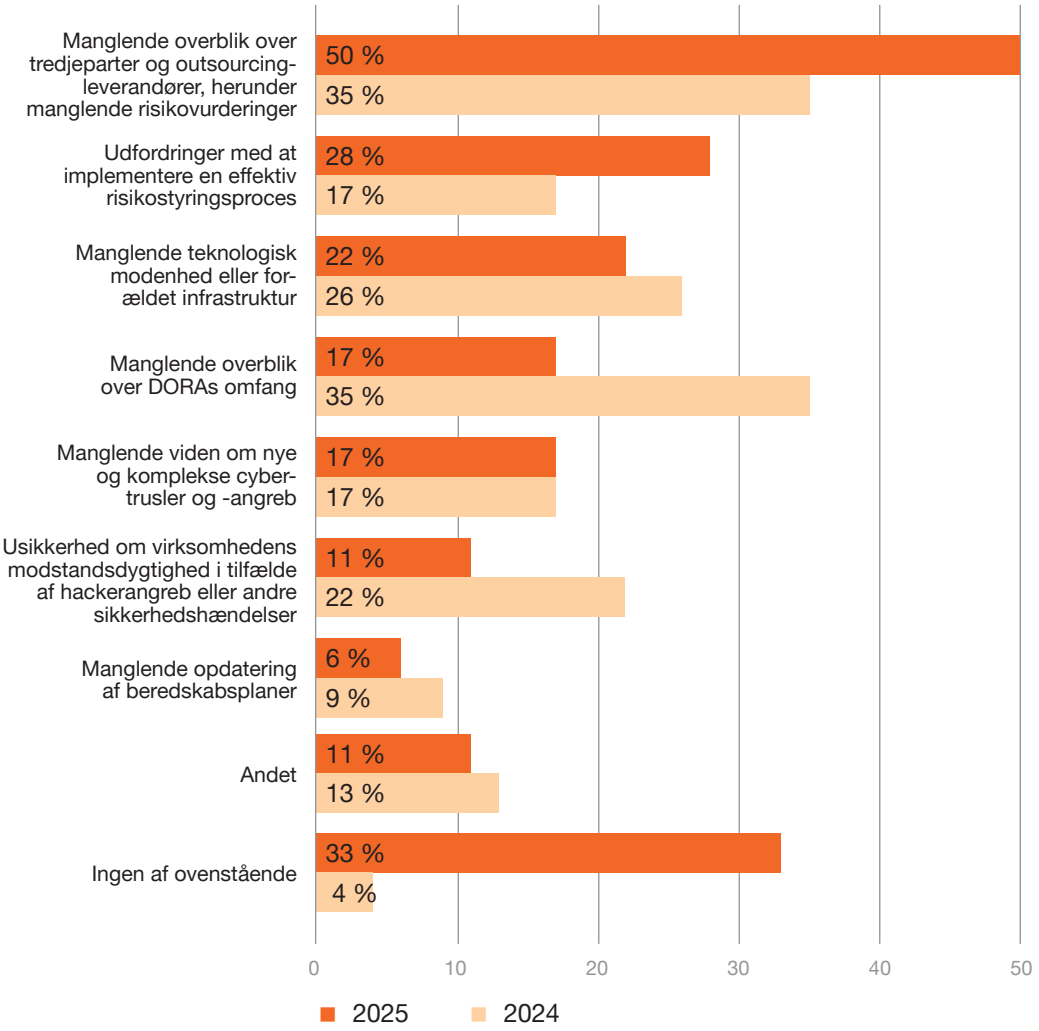
Tallene afspejler en stigende bekymring for forsyningskædens sikkerhed og manglende transparens mellem virksomheder og leverandører. Disse faktorer udgør væsentlige barrierer for efterlevelse af kravene i både DORA og NIS 2.

Hvilke af følgende ser du som barrierer for, at din virksomhed* kan leve op til kravene i NIS 2-direktivet?



*) Kun virksomheder, der har angivet, at de er omfattet af NIS 2.

Hvilke af følgende ser du som barrierer for, at din virksomhed* kan leve op til kravene i DORA-forordningen?



*) Kun virksomheder, der har angivet, at de er omfattet af DORA.

PwC's 2026 Global Digital Trust Insights-undersøgelse

I PwC's 2026 Global Digital Trust Insights-undersøgelse angiver 27 % af de adspurgte ledere, at sikkerhedsbrud hos tredjeparter er den cybertrussel, deres organisationer er mindst forberedte på at håndtere. Undersøgelsen fremhæver en væsentlig udfordring, idet virksomheder har begrænset kontrol over risici, der opstår uden for deres egne systemer. Dette gør det vanskeligt at beskytte sig mod trusler fra eksterne samarbejdspartnere og leverandører.

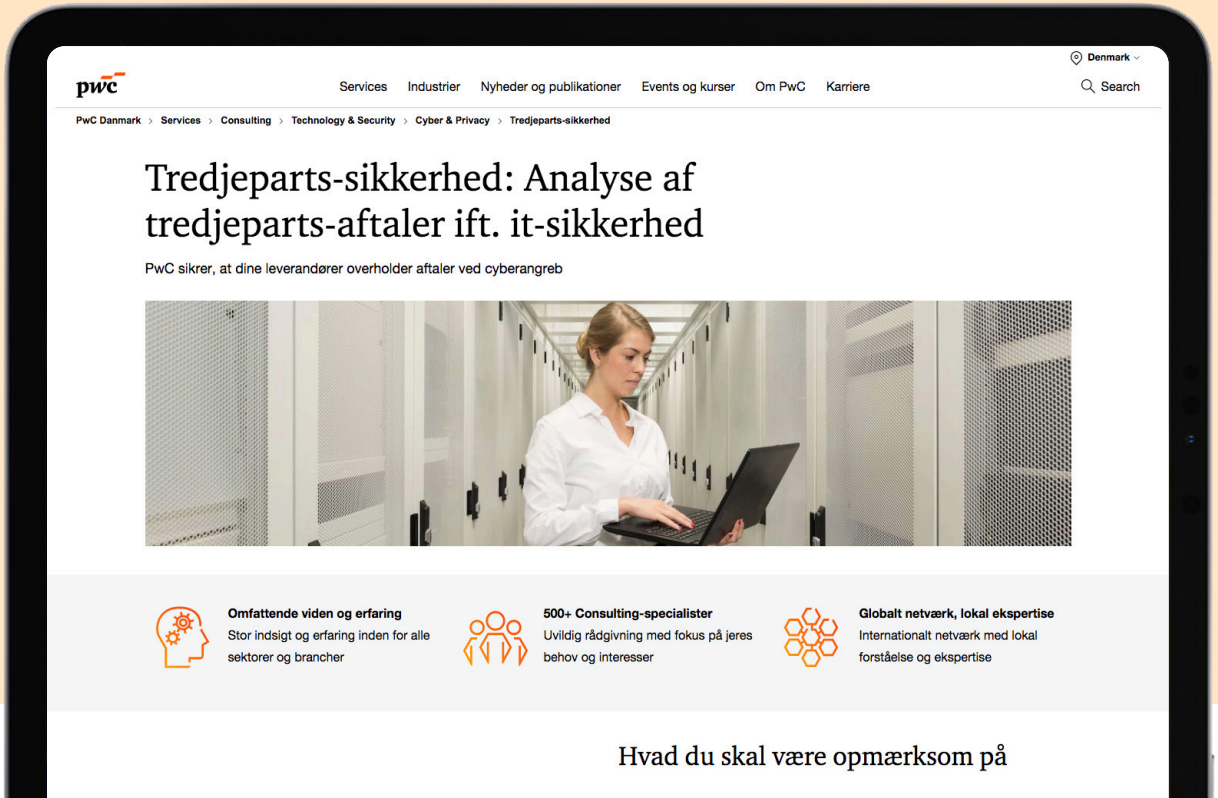
1) PwC's 2026 Global Digital Trust Insights-undersøgelse blandt 3.887 forretnings- og teknologiledere fra 77 lande afslørede betydelige mangler, som virksomheder skal udbredre for at opnå cybersikker modstandsdygtighed.

PwC erfarer

Effektiv leverandørstyring kræver et beredskab, hvor tekniske og forretningsmæssige funktioner samarbejder om at beskytte virksomheden mod trusler, der opstår uden for egne systemer. Virksomheder, der outsourcer deres ydelser, bør stille specifikke krav til leverandørernes cybersikkerhed og løbende få vished for, at leverandøren efterlever disse krav. Virksomhederne bør specifikt følge op på deres leverandørers evne til at håndtere sikkerhedshændelser.

PwC anbefaler, at man gennemgår kontrakter og SLA'er med fokus på adgangsforhold. En systematisk tilgang til outsourcing og tredjepartsstyring er afgørende for at kunne leve op til regulatoriske krav og beskytte forretningen mod cybertrusler.

Læs mere om PwC's anbefalinger til tredjepartssikkerhed og om, hvordan vi kan hjælpe dig.



Cyber-sikkerhed på bestyrelsens dagsorden: En positiv udvikling

Cybercrime Survey 2025 viser, at cybersikkerhed i stigende grad er blevet en integreret del af bestyrelsens arbejde.

76 %

af respondenterne svarer, at cyber-sikkerhed indgår som en fast del af bestyrelsens årshjul.

Cybersikkerhed som fast punkt i bestyrelsens årshjul

Hele 76 % af respondenterne svarer, at cybersikkerhed indgår som en fast del af bestyrelsens årshjul. Det svarer til tre ud af fire virksomheder og indikerer en styrket strategisk prioritering af området på ledelsesniveau. Der er tale om en stigning fra 70 % i 2024, som understreger en styrket strategisk prioritering af cybersikkerhed på ledelsesniveau.

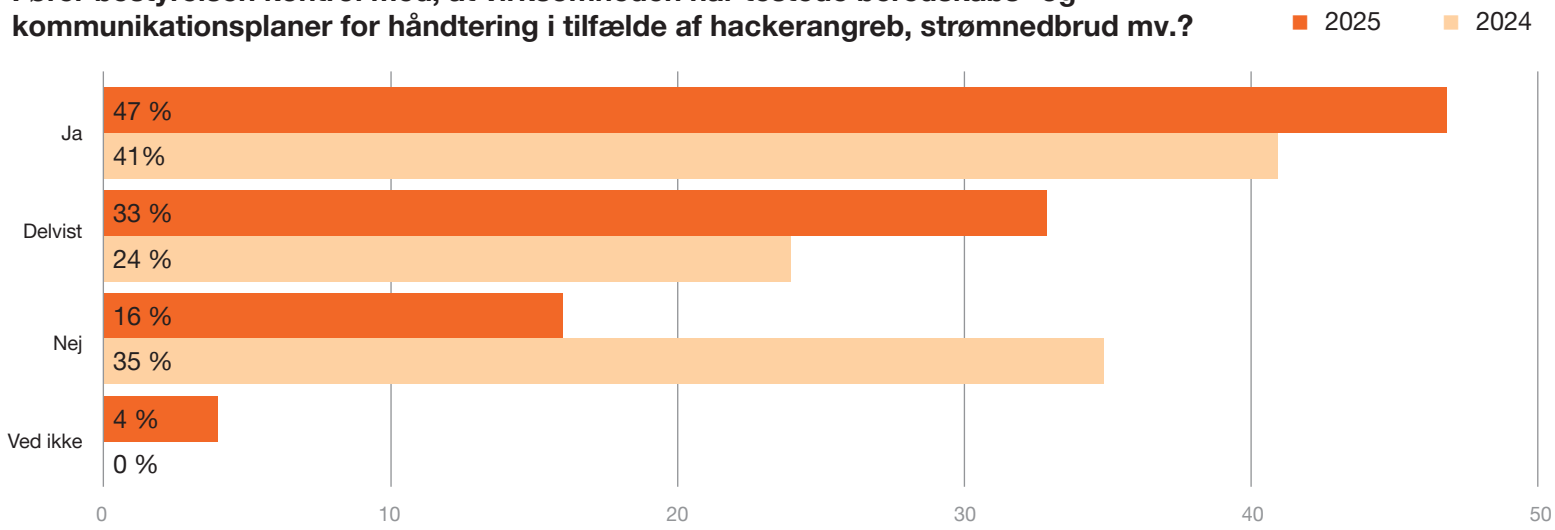
Samtidig har indførelsen af EU-direktiverne NIS 2 og DORA øget kravene til virksomhedernes cybersikkerhed, hvor bestyrelsen nu har et direkte ansvar for at sikre tilstrækkelig styring af digitale risici og operationel robusthed. Dette skifte betyder, at cybersikkerhed i dag ikke længere er et isoleret teknisk anliggende, men en central ledelsesopgave for virksomhedens øverste niveau.

Bestyrelsens kontrol med beredskabsplaner

Cybersikkerhed har fortsat en central placering på bestyrelsesniveau i dansk erhvervsliv. Cybercrime Survey 2025 viser en positiv udvikling i bestyrelsens involvering i virksomhedens beredskab. 47 % af respondenterne angiver, at bestyrelsen fører kontrol med, at der findes testede beredskabs- og kommunikationsplaner. Det er en stigning fra 41 % i 2024.

Samtidig er andelen, der svarer "nej" til, om bestyrelsen fører kontrol med beredskabs- og kommunikationsplaner, faldet markant fra 35 % i 2024 til 16 % i 2025. Denne udvikling tyder på, at flere bestyrelser har fået øget fokus på beredskab som en central del af agendaen. Dette afspejler en positiv, stigende erkendelse af, at ledelsesmæssigt ansvar også omfatter forberedelse og reaktionsevne i tilfælde af sikkerhedsbrud.

Fører bestyrelsen kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner for håndtering i tilfælde af hackerangreb, strømnedbrud mv.?

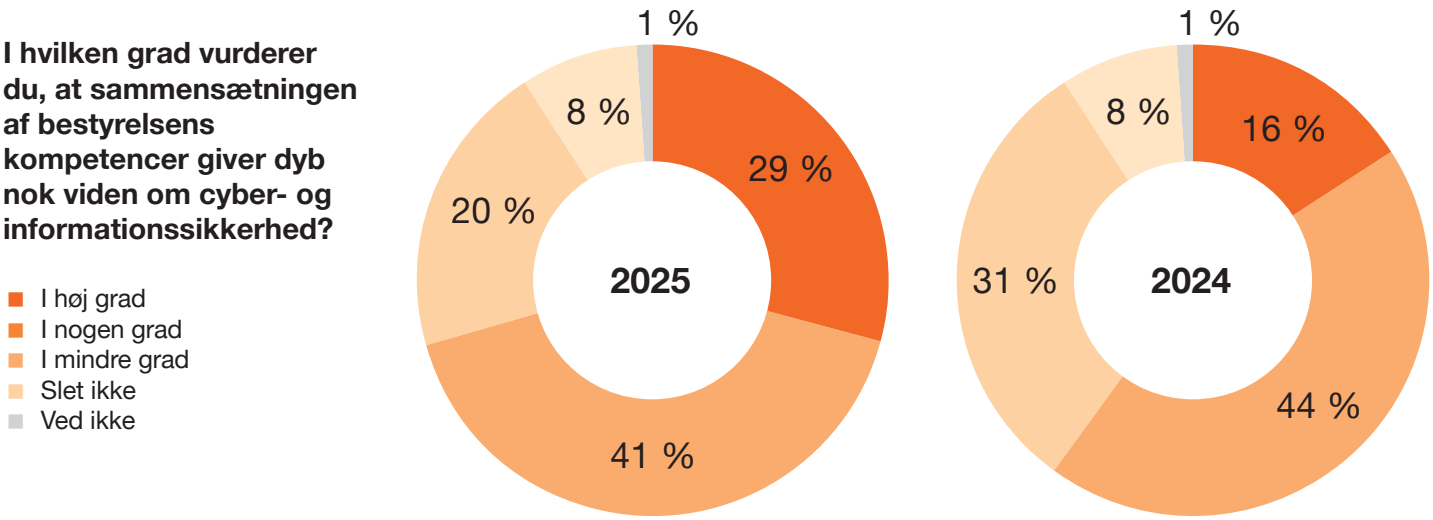


Positiv udvikling i bestyrelsens cybersikkerhedskompetencer

Undersøgelsen viser en positiv udvikling i opfattelsen af bestyrelsens kompetencer inden for cyber- og informationssikkerhed. I 2025 vurderer 29 % af respondenterne, at bestyrelsen i høj grad har kompetencer, der giver dyb nok viden om cyber- og informationssikkerhed, hvilket er en stigning fra 16 % i 2024.

Samtidig er andelen, der mener, at bestyrelsen kun i mindre grad besidder relevante kompetencer, faldet fra 31 % til 20 %. Denne udvikling tyder på, at flere virksomheder har haft fokus på at styrke bestyrelsens kompetencer inden for cybersikkerhed.

I hvilken grad vurderer du, at sammensætningen af bestyrelsens kompetencer giver dyb nok viden om cyber- og informationssikkerhed?



29 %

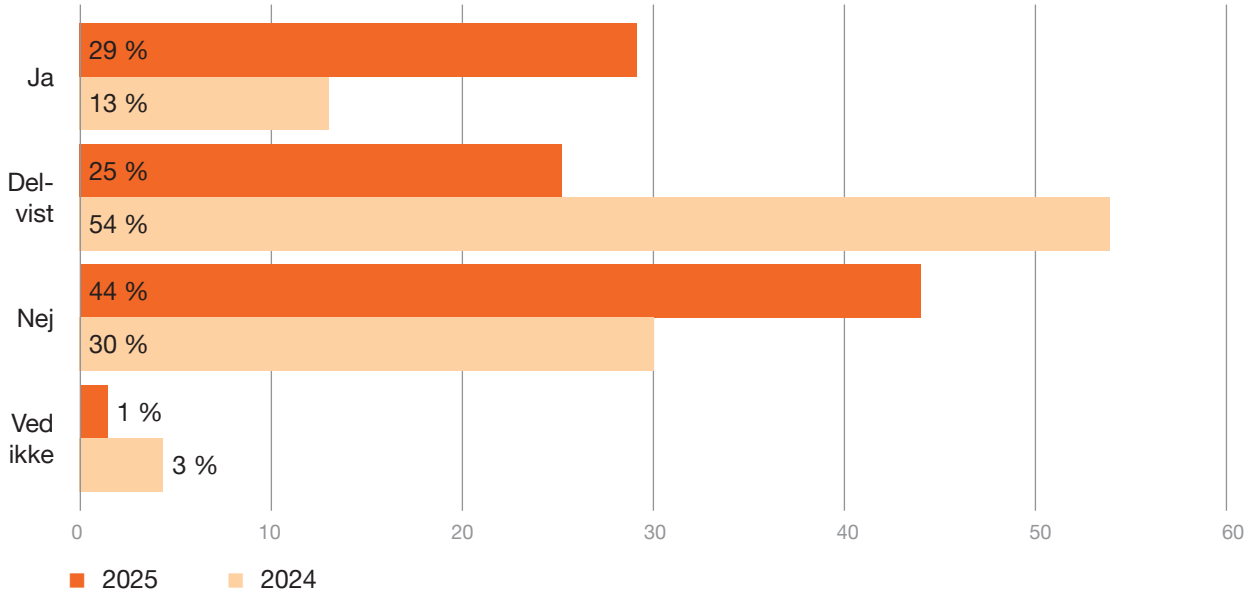
af respondenterne vurderer, at bestyrelsen i høj grad har kompetencer, der giver dyb nok viden om cyber- og informationssikkerhed.

Andelen, der mener, at bestyrelsen kun i mindre grad besidder relevante kompetencer, er faldet fra 31 % til 20 %. Denne udvikling tyder på, at flere virksomheder har haft fokus på at styrke bestyrelsens kompetencer inden for cybersikkerhed.

20 %

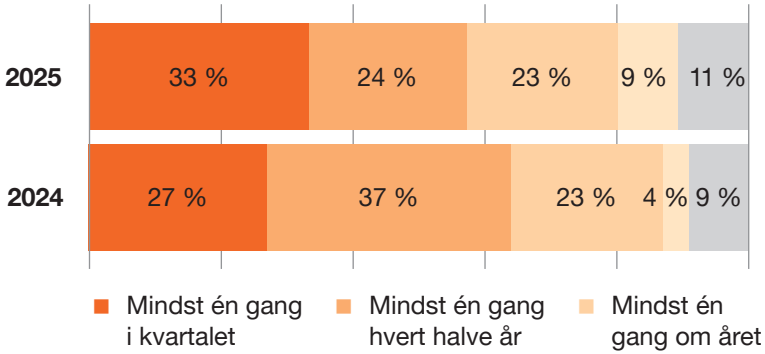
af respondenterne vurderer, at bestyrelsen i mindre grad har kompetencer, der giver dyb nok viden om cyber- og informationssikkerhed.

Modtager bestyrelsen træning i cyber- og informationssikkerhed?

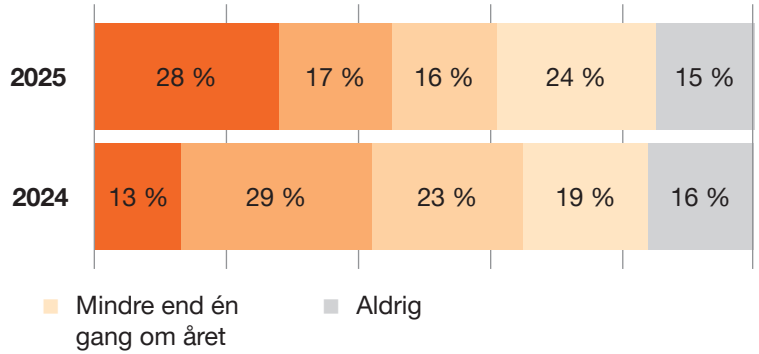


Indførelsen af EU-direktiverne NIS 2 og DORA har øget kravene til virksomhedernes cybersikkerhed, hvor bestyrelsen nu har et direkte ansvar for at sikre tilstrækkelig styring af digitale risici og operationel robusthed.

Hvor ofte modtager og behandler bestyrelsen information vedrørende cyberrisici?



Hvor ofte behandler bestyrelsen cyberhændelser?



AI er fortsat en markant faktor i arbejdet med cyber-sikkerhed

I takt med den stigende digitalisering og kompleksiteten af cybertrusler intensiveres behovet for avancerede AI-værktøjer til at beskytte virksomheder.

AI spiller en stadig vigtigere rolle i cybersikkerhedsarbejdet, og i 2025 anvender eller planlægger hele 72 % af virksomhederne at bruge AI – en stigning fra 61 % i 2024. Denne udvikling afspejler AI's voksende betydning som en strategisk komponent i kampen mod cyberangreb.

De områder, hvor virksomheder planlægger at bruge AI i arbejdet med cybersikkerhed, er fortsat primært inden for identifikation af mulige trusler samt opdagelse af netværksangreb, malware og anomalier.

Mange anvender også AI til at beskytte virksomhedens aktiver og til at reagere på hændelser gennem analyse af logdata og hændelsesspor. Kun 5 % af respondenterne vurderer stadig, at AI kan være nyttig til reetablering af systemer efter en hændelse.

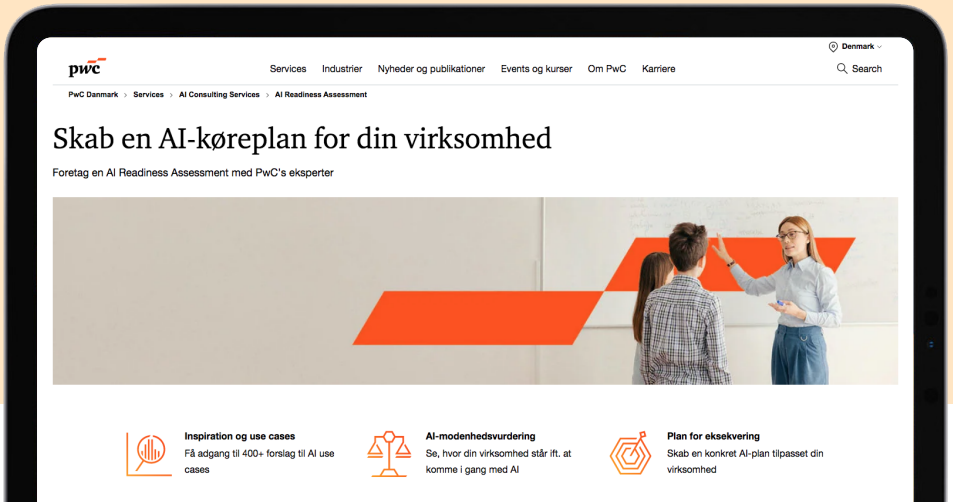
PwC erfarer

Virksomhedsledere har mange grunde til at være begejstrede for de muligheder, som især generativ AI kan tilbyde. Men som med enhver ny teknologi medfører det også potentielle risici og nye lovgivningskrav, der skal overholdes. For at hjælpe din virksomhed med at udnytte generativ AI's store potentiale, samtidig med at I effektivt håndterer risici og overholder lovgivningsmæssige krav, har vi i PwC udviklet rammeværket "Responsible AI".

Læs mere om, hvordan PwC arbejder med "Responsible AI".

I PwC hjælper vi virksomheder med at levere en plan med konkrete input til anvendelse og implementering af AI. Vi har fokus på, hvad det kræver teknisk – og hvordan virksomheden skaber forandringen. PwC's eksperter udarbejder en AI-plan, hvor vi sammen dykker ned i de aktuelle behov og på baggrund af analyser og interviews afdækker, hvor og hvordan din virksomhed kan få gavn af AI. Udbyttet for dig og din virksomhed bliver en skræddersyet plan med konkrete anbefalinger, handlinger og mål, I kan eksekvere på fra første dag.

Læs mere om PwC's AI Readiness Assessment.



11 % **af virksomhederne har i 2025 oplevet en cyberhændelse, hvor angriberen har anvendt AI-teknologi – mere end en fordobling fra 5 % i 2024. Det vidner om en markant udvikling i trusselsbilledet, hvor AI i stigende grad bliver en del af de cyberkriminelles værktøjskasse.**

Om undersøgelsen

405 danske topledere, sikkerhedschefer og fagspecialister har deltaget i PwC's Cybercrime Survey 2025. Denne rapport sætter fokus på cybersikkerhed i dansk erhvervsliv og hos offentlige institutioner.

Undersøgelsen er igen i år gennemført med opbakning fra Finans Danmark, It-branchen, Dansk Erhverv, Styrelsen for Samfundssikkerhed, KITA, Rådet for Digital Sikkerhed, ISACA, Dansk IT, Bestyrelsesforeningen, Punktum DK og Computerworld.

Analysen bygger på onlinebesvarelser. Respondenterne er blevet stillet en række spørgsmål inden for cyber- og informationssikkerhed. Målingens spørgsmål og svarmuligheder er udarbejdet af PwC, og onlinespørgeskemaet er udsendt i samarbejde med førnævnte organisationer.

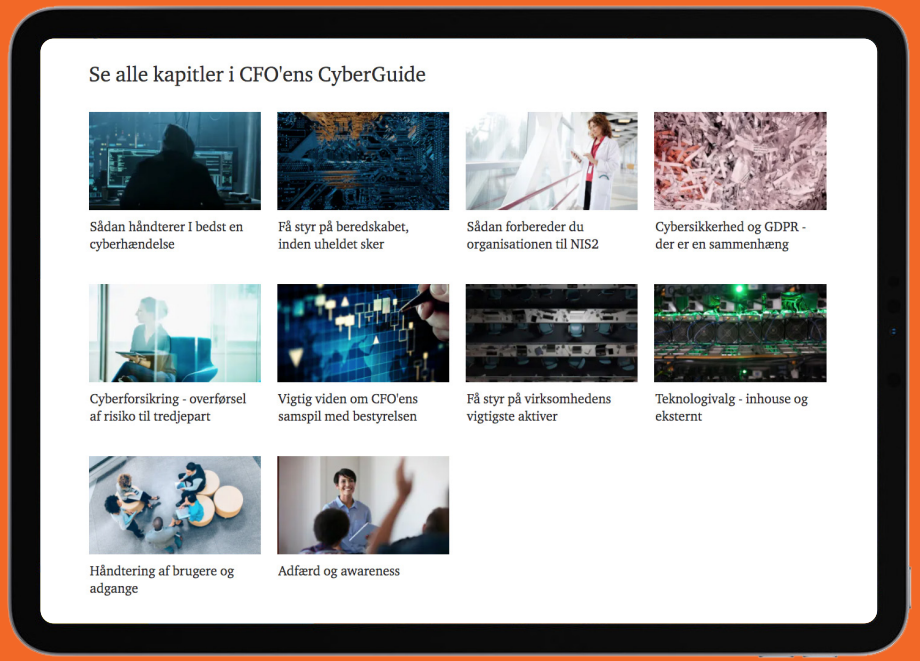
405

danske topledere, sikkerhedschefer og fagspecialister har deltaget i PwC's Cybercrime Survey 2025.

Få flere tips til cyberberedskabet

Er du CFO eller en del af ledelsen? CFO'ens Cyberguide tager dig igennem de trin, der ligger i at opbygge et strategisk cyberberedskab i din virksomhed.

Læs mere i CFO'ens Cyberguide



Tjekliste

I PwC vil vi gerne hjælpe virksomheder med at sikre sig bedst muligt mod cybertrusler – både før, under og efter et angreb. Da løsningerne kan være mange og ofte komplekse, har PwC udarbejdet denne liste, der kan hjælpe virksomheder med at tage stilling til nogle af de vigtigste indsatsområder inden for cyber- og informationssikkerhed.

Governance, risk og compliance	
	Har I etableret et formelt sikkerhedsudvalg med repræsentanter fra virksomhedens topledelse?
	Er øvrige roller for cyber- og informationssikkerhed defineret, allokeret og kommunikeret?
	Arbejder I struktureret med risikovurdering ud fra sikkerhedstrusler, sårbarheder og konsekvens for forretningen?
	Rapporteres virksomhedens sikkerhedsstatus jævnligt/løbende til virksomhedens direktion/bestyrelse?
	Omfatter arbejdet med sikkerhed både informationssikkerhed og cybersikkerhed? Læs mere om ISO 27001 og NIS 2 **her.**
	Har I implementeret relevante foranstaltninger til overholdelse af GDPR (persondataforordningen)?
	Arbejder I proaktivt med henblik på fortsat overholdelse af kravene i GDPR?
Processer	
	Har I foretaget en vurdering af jeres robusthed mod cybertruslerne (cyber assessment)?
	Har I dokumenteret og kommunikeret processer for alle områder af sikkerhed?
Adfærd	
	Er der etableret et program for løbende uddannelse og oplysning af medarbejderne om sikkerhed? Læs mere **her.**
Validering	
	Gennemfører I løbende test i forhold til identifikation af sårbarheder i jeres infrastruktur og systemer?
	Har I fastlagt og afprøvet en Incident Response-proces? Læs mere **her.**
	Har I testet jeres beredskabsplaner for cyberhændelser? Læs mere **her.**
Arkitektur	
	Har I udarbejdet en plan for implementering af hensigtsmæssig sikkerhedsteknologi?
	Har I fastlagt en proces for privacy by design, herunder adgang til persondata? Læs mere **her** og **her**.

Kontakt

Vi vil meget gerne i dialog med dig om resultaterne fra årets Cybercrime Survey. Kontakt en af PwC's eksperter for en uforpligtende snak om dine konkrete udfordringer og behov.

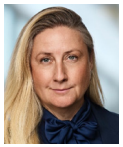
Læs mere om vores ydelser inden for cyber- og informationssikkerhed på pwc.dk/cyber, eller scan QR-koden.

Mads Nørgaard Madsen
Partner, Leder af Consulting
T: 2811 1592
E: mads.norgaard.madsen@pwc.com

Christian Kjær
Partner, Cyberrisikostyring
T: 5132 1270
E: christian.kjaer@pwc.com

Marc Jerner
Partner, Security Technology
T: 4099 4698
E: marc.jerner@pwc.com

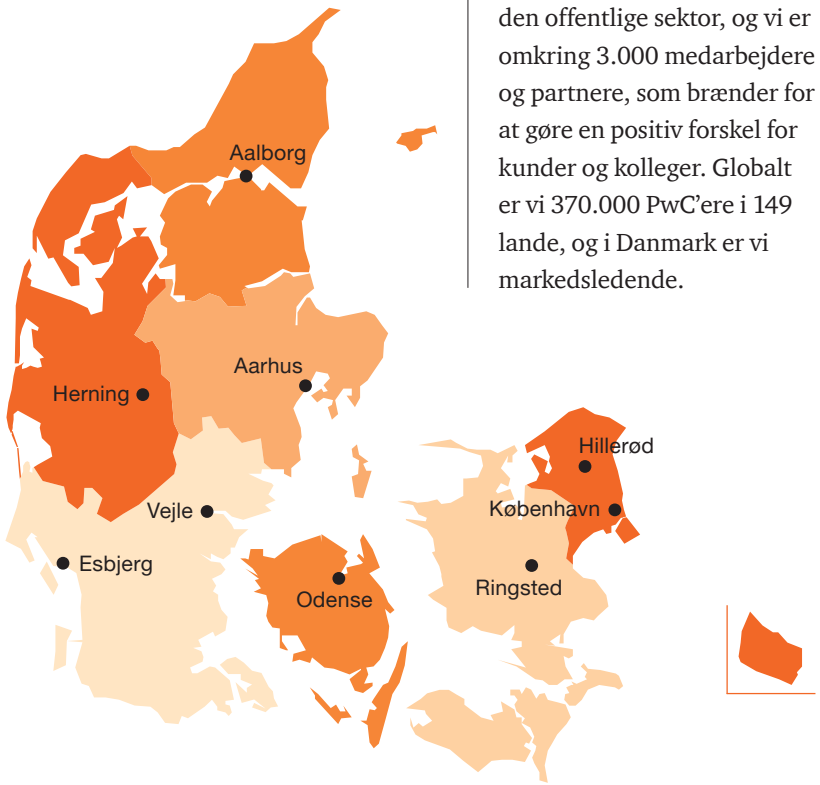
Morten Friis
Partner, Security Technology
T: 5215 0258
E: morten.friis@pwc.com



Malene Fagerberg
Partner, Cyberrisk & Regulation
T: 2567 9447
E: malene.fagerberg@pwc.com

William Sharp
Partner, Operationel Technology
T: 4040 1074
E: william.sharp@pwc.com

Kenneth Studsgaard Pedersen
Partner, Cyberrisikostyring
T: 3136 1073
E: kenneth.studsgaard.pedersen@pwc.com



Om PwC

I PwC arbejder vi for at styrke tilliden i samfundet og være med til at løse væsentlige problemstillinger. Det gør vi med udgangspunkt i vores viden inden for revision, skat og rådgivning.

Vores kunder kommer fra alle dele af erhvervslivet og den offentlige sektor, og vi er omkring 3.000 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi 370.000 PwC'ere i 149 lande, og i Danmark er vi markedsledende.

Cyber Incident Response-team

PwC hjælper kunder med at forebygge og håndtere cybersikkerhedshændelser

Vi har etableret en central cyberhotline for kunder, så du har mulighed for at få akut hjælp. PwC's team af eksperter hjælper med at skabe overblik over indsatsområder i forhold til den konkrete trussel, og vores cyberforensics-specialister identificerer angrebets art og de udnyttede sårbarheder. Derefter implementerer vi forbedringer af sikkerheden og udarbejder en rapport til brug for bl.a. ledelsen, forsikringen, Datatilsynet og politiet.

PwC's cyberhotline

70 222 444

Læs mere: pwc.dk/response

pwc

pwc.dk/cyber